UDC 003.26:004.056.55

SOFTWARE FOR RESEARCH CRYPTOGRAPHIC HASH-FUNCTION USING CELLULAR AUTOMATA

Yuriy Nester
Ternopil National Economic University, Master's Degree student

I. Formulation of the problem

Exhaustive of all possible scheme variations, that will work on quantum phenomena provides an optimal solution, but has exponential complexity and require too much time [1]. Therefore, the development of methods for the synthesis of return schemes that would provide quasi-optimal result at polynomial computational complexity is urgent and important task of the scientific and practical points of view.

II. The purpose of the work

The purpose of research is the development and implementation of a software algorithm for hashing s3 rounded functions on cellular automata and research their scattering properties.

III. Hash Algorithm SHA-3 standard

According to the definition of the properties of mixing, which is characteristic for hash function, at any hash value argument not differ from computing point of view of the line bits, what are evenly distributed in the function, that belongs to the general population for evenly distributed numbers. In this we obtain a powerful feature called Random Oracle, which has three properties: it is a deterministic, efficient and ensures evenly distribution of the resulting values. This function considered hypothetical because each known computing models are powerful [2].

According to [3] random oracle – is an abstract black box, which has infinite memory and runs the following algorithm:

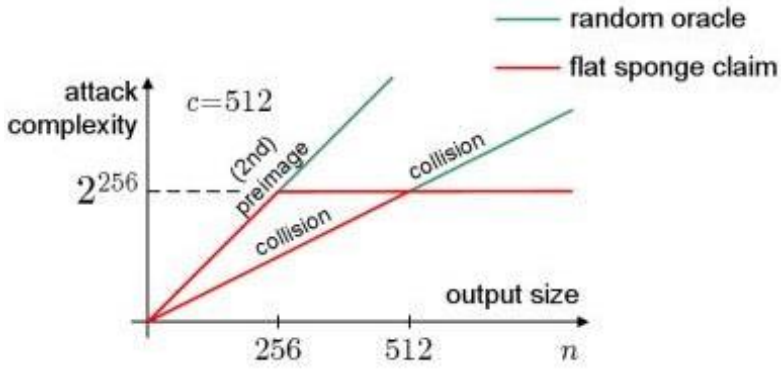

Figure 1- Random Oracle

- Gets the input line and verifies that worked with him before.
- If not, generating true random number and stores a couple of line - number.

If so, issues previously stored number for that line.

This design is similar to the hash function, with the difference that the connection between the hashed line and the result can not be calculated. [1].

Random oracle, according to [1], – is idealized function that describs the machine with virtually infinite storage capacity that for any request can issue a perfectly random number and remember a couple of "challenge-response". If the same request is repeated once, the answer will not be generated again, as evidenced from a saved list. If permutation f, which underlies the design sponge, ideal, then hash function not differ from a random oracle, and therefore any possible attacks will not work.

These theoretical results based on one of the irrefutable evidence of similarity to a random oracle in the SHA-3 competition, provide new opportunities for the practical use of a simple hash function Keccak as virtually universal cryptoprimitive [2].

Conclusion

As a result of research work using C++ developer tools was created cryptographic sponge-based cellular automata and researched the possibility of using cellular automata in cryptographic hash functions.

References

1. Why Keccak is so cool and why it was chosen as the new SHA-3. [Electronic resource] - Access mode: https://habrahabr.ru/ post / 168707
2. Keccak hash function and Sponge design as a universal crypto-primitive. [Electronic resource] - Access mode: https://www.pgpru.com/biblioteka/statji/keccaksponge.
3. Schneier B. Applied cryptography. Protocols, algorithms, source texts in C language. / B. Schneier. - Moscow: Triumph, 2009. - 806 p.

УДК 004.056

ПРОЕКТУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ПРОСОЧУВАННЯ ІНФОРМАЦІЇ В ПЕРЕДАНОМУ ПОТОЦІ ДАНИХ

Божко Н.В. [1], Моргун Ю.А.[2]

Коледж Миколаївського національного університету імені В.О.Сухомлинського

[1] викладач; [2] студент

I. Постановка проблеми

Комерційний інтерес на сьогодні є метою несанкціонованого збору інформації. На жаль в нашій країні на теперішній момент не досить належний рівень інформаційної безпеки корпоративних мереж. Фактичний та потенційно можливий матеріальний збиток компаній досить високий від прихованого просочування інформації.

Системи безпеки в основному повинні обмежувати допуск користувачів до інформаційних ресурсів, визначати їх повноваження, вміти розпізнавати несанкціоновані вторгнення в мережеву інфраструктуру, прогнозувати аварійні ситуації та усувати їх наслідки часткової втрати або тривалого блокування ресурсів.

Для того щоб важлива інформація надійно була захищена, вкрай необхідно забезпечити її цілісність даних та конфіденційність.

II. Мета роботи

Метою дослідження є проектування системи виявлення просочування інформації в переданому потоці даних у вигляді програмного модуля виявлення текстових областей в графічних файлах для вирішення завдань запобігання просочування конфіденційної інформації.

III. Розробка та використання системи

На підставі вищесказаного, було прийняте рішення створити програмний модуль, який мав би можливість виявлення в графічних файлах передачу текстових областей. За допомогою даного модуля стане можливим поліпшення комплексного захисту автоматизованої корпоративної системи, її інформаційної безпеки та запобігання несанкціонованого поширення конфіденційної інформації в графічних файлах.

Функції розробленого модуля: аналіз графічних файлів, виявлення текстових областей, які відповідають заданим критеріям; вивід звіту про досліджені графічні файли; виділення потенційно «небезпечних» зображень.

Підсистема виводить звіт про дослідження графічних файлів, результати дослідження залежать від заданих критеріїв.

Програмний модуль знаходить текстові області в графічних файлах, які можуть містити в собі конфіденційну інформацію та повідомляє про них для подальшого їх дослідження іншими модулями системи захисту.

Перевагою даного модуля є швидке знаходження необхідних текстових областей. Це дозволяє передавати на подальше дослідження системи захисту для розпізнавання образів на предмет наявності конфіденційної інформації тільки ті файли, в яких містяться дозволені текстові області. Це допомагає пришвидшити оброблення графічної інформації, додає властивість комплексності в цілому всієї системи.

В основу розробки блок-схеми алгоритму роботи системи взяті існуючі алгоритми виявлення текстових областей, а саме алгоритм «Швидке і ефективне текстове виявлення» (рис.1).